Security of EPR-based Quantum Key Distribution using three bases

Hitoshi Inamori
Centre for Quantum Computation, Oxford University

August 19, 2000

Abstract

Modifications to a previous proof of the security of EPR-based quantum key distribution are proposed. This modified version applies to a protocol using three conjugate measurement bases rather than two. A higher tolerable error rate is obtained for the three-basis protocol.

1 Introduction

A modified version of a proof of the security [1] of EPR-based quantum key distribution is proposed. Based on the works [2, 3], this modified version applies to a protocol using three conjugate measurement bases rather than two. Only modified parts of the proof are presented here. The framework of our study and the remaining parts of the proof can be found in [1].

2 The protocol

We describe the quantum key distribution protocol under consideration. It is a variation of the protocol described in [1] using three conjugate measurement bases rather than two. In this variation, the source is supposed to emit pairs of photons with orthogonal polarisations. As a consequence, Alice's bits and Bob's bits are anticorrelated when no error occurs.

Protocol setup

Alice and Bob specify:

- m, the length (in bits) of the private key to be generated.
- ϵ, the maximum threshold value for the error rate during the quantum transmission ($\epsilon < 1/4$).
- τ, a security constant such that $\frac{\epsilon}{1-\epsilon} < \frac{\epsilon}{1-\epsilon} + \tau < 1$.
- the security parameter r. It must be large enough so that Alice and Bob can find a binary matrix K of size $m \times r$ such that any linear combination of rows of K that contains at least one row of K has weight greater than $d_K = \left(\frac{\epsilon}{1-\epsilon} + \tau\right) r$. Alice and Bob choose one

such matrix K. Shannon's coding theorem tells that for asymptotic values of m, such matrix can be found if r obeys the inequality:

$$\frac{m}{r} \leq 1 - h\left(\frac{1}{2}\frac{\epsilon}{1-\epsilon} + \frac{\tau}{2}\right).$$

- An error reconciliation scheme for strings of length $s = \left\lfloor \frac{r}{1-\epsilon} \right\rfloor$ bits as specified in [1].
- n, the number of pairs of photons to be sent to the legitimate parties. A good choice for n is $\left\lceil \frac{r}{\frac{1-\epsilon}{3} - \tau_S} \right\rceil$ where τ_S is a small but strictly positive constant.

Quantum transmission

- A source sends a sequence of n photons to Alice and another sequence of n photons to Bob. It is assumed that ideally, for each $i \in \{1 \dots n\}$, the source emits a pair of photons in the state:

$$|\Psi^-\rangle = \frac{|\,0\rangle_0 |\,1\rangle_0 - |\,1\rangle_0 |\,0\rangle_0}{\sqrt{2}}$$

  and that Alice's i-th photon is the first photon of this pair, and Bob's i-th photon is the second photon of this pair. The kets $|\,0\rangle_0$ and $|\,1\rangle_0$ form an orthonormal basis "0" of the Hilbert space describing the polarisation of one photon. The kets $|\,0\rangle_1 = \frac{|\,0\rangle_0 - |\,1\rangle_0}{\sqrt{2}}$ and $|\,1\rangle_1 = \frac{|\,0\rangle_0 + |\,1\rangle_0}{\sqrt{2}}$ form its first conjugate basis "1". The second conjugate basis "2" is formed by the kets $|\,0\rangle_2 = \frac{|\,0\rangle_0 + i|\,1\rangle_0}{\sqrt{2}}$ and $|\,1\rangle_2 = i\frac{|\,0\rangle_0 - i|\,1\rangle_0}{\sqrt{2}}$.

  As in [1], the source needs not to be trusted and can be under Eve's control. The only assumption is that Alice and Bob receive a sequence of n single photon signals on each side.
- We assume that the measurement devices of Alice and Bob have efficiency one. For each $i \in \{1 \dots n\}$,
  1. Alice picks randomly a basis $a_i \in \{0, 1, 2\}$ with uniform probability distribution. Alice measures her i-th photon in the basis a_i, obtaining the outcome $\alpha_i \in \{0, 1\}$, corresponding to the state $|\,\alpha_i\rangle_{a_i}$.
  2. Similarly, Bob picks randomly and independently of Alice a basis $b_i \in \{0, 1, 2\}$ with uniform probability distribution. Bob measures his i-th photon in the basis b_i, obtaining the outcome $\beta_i \in \{0, 1\}$, corresponding to the state $|\,\beta_i\rangle_{b_i}$.

Sifting

Alice and Bob compare publicly their bases $\vec{a}$ and $\vec{b}$. We denote by $\vec{d}$ the vector in $\{0, 1, 2\}^n$ defined by $d_i = b_i - a_i \pmod 3$ for all $i \in \{1 \dots n\}$. If the number of indexes $i \in \{1 \dots n\}$ such that $a_i = b_i$ is greater than or equal to s then the sifted set S is the set of the first s such indexes. Otherwise the validation test is failed. The bit strings α_S and $\neg\beta_S$ are the sifted keys, where for any vector $\vec{x} \in \{0, 1\}^n$, we denote by $\neg\vec{x}$ the vector whose i-th entry is $1 + x_i \pmod 2$ for all $i \in \{1 \dots n\}$.

Error correction

Alice and Bob perform the error correction on their sifted keys α_S and $\neg\beta_S$ as specified in the protocol setup. The error set E is the set of indexes i in S in which an error is found, that is, $\alpha_i = \beta_i$. The error vector $\vec{e}$ is the vector in $\{0,1\}^s$ giving the positions of the errors ($\forall i \in \{1,\ldots,s\}$, $e_i = 1$ if and only if $\alpha_i = \beta_i$). We denote by e the size of the set E. The validation test is passed if $e < \epsilon s$, otherwise it is failed. If the validation test is passed, then the reconciled set R is the set of the first r indexes $i \in S \setminus E$. Therefore $|R| = r$ and $\forall i \in R$, $a_i = b_i$ and $\alpha_i = \neg\beta_i$. Alice and Bob obtain with high probability an identical string of bits $\alpha_R \in \{0,1\}^r$, called the reconciled key.

Privacy amplification

The private key is defined as:

1. $\vec{\kappa} = K\alpha_R \pmod 2$ if the validation test is passed.
2. an m-bit string $\vec{\kappa}$ picked randomly by Alice with uniform probability distribution each time the validation test is failed.

3 Privacy of the protocol

The privacy of the three-basis protocol is stated and the achievable key-creation rate discussed.

Property 1 *The protocol described above offers perfect privacy: for any eavesdropping strategy chosen by a possible eavesdropper, the conditional entropy of the private key $\vec{\boldsymbol{\kappa}}$ given the eavesdropper's view $\boldsymbol{v}$ is bounded from below by:*

$$H(\vec{\boldsymbol{\kappa}}|\boldsymbol{v}) \geq m - 2\left(m + \frac{1}{\ln 2}\right)\left(\theta(r) + 2\sqrt{\theta(r)}\right),$$

where

$$\theta(r) = e^{-\frac{1}{16}\tau^3 r}.$$

The above bound applies for any value of the security parameter r such that the matrix K specified in the protocol exists.

Therefore, for asymptotic values of the security parameter r, a net gain in shared private bits can be obtained if:

$$1 - h\left(\frac{1}{2}\frac{\epsilon}{1-\epsilon}\right) - \frac{1}{1-\epsilon}h(\epsilon) > 0.$$

since $sh(\epsilon)$ bits are required for the one-time pad encryption during the error reconciliation, as in [1].

In comparison, we proved that for the original protocol using two measurement bases only, a net gain in shared private bits can be obtained if:

$$1 - h\left(\frac{\epsilon}{1-\epsilon}\right) - \frac{1}{1-\epsilon}h(\epsilon) > 0.$$

Therefore, the three-basis protocol seems to be more robust than the original protocol. However, one must realise that a given threshold value on the error rate gives different physical constraints on the quantum channel depending on whether two-basis or three-basis protocol is used. Whether the two-basis or the three-basis protocol is more robust and efficient depends on the technology chosen to implement the transmission and the reception of the quantum signals.

4 Proof of the privacy

The proof of the above result is given. It is mainly identical to the proof proposed in [1] for the original protocol. Therefore, only parts that are different from this previous proof are detailed. The main difference between the previous proof and this proof resides in Section 4.3.

4.1 Notations

We define the notations used throughout the proof. They are similar to the ones used in [1], but the indexes for Bell states have been modified. The notations have been adapted to deal with three bases.

Classical data

We denote by $C = (\vec{a}, \vec{b}, \vec{\alpha}, \vec{\beta})$ the classical data Alice and Bob generate during the protocol (after the setup). We denote by $P = (\vec{a}, \vec{d}, \vec{e})$ the data that are publicly announced by Alice and Bob during the protocol. For any possible P, we denote by $\mathcal{C}_P$ the set of values for the classical data that are compatible with the public announcement of P. That is, for a given $P = (\vec{a}, \vec{d}, \vec{e})$,

$$\begin{aligned} \mathcal{C}_P \quad = \quad & \{C' = (\vec{a}', \vec{b}', \vec{\alpha}', \vec{\beta}') \,:\, \vec{a}' = \vec{a}, \\ & \forall i,\, b'_i = a_i + d_i \pmod 3 \\ & \forall i \in E,\, \alpha'_i = \beta'_i \text{ and } \forall i \in S \setminus E,\, \alpha'_i = \neg\beta'_i \\ & \text{where } S \text{ and } E \text{ are given by } \vec{d} \text{ and } \vec{e}.\}. \end{aligned}$$

Given a possible P and a value for the private key $\vec{\kappa}$, we define $\mathcal{C}_{P,\vec{\kappa}}$ as the set of values for the classical data that are compatible with the public announcement of P and generation of $\vec{\kappa}$ for the private key. That is, for a given $P = (\vec{a}, \vec{d}, \vec{e})$,

$$\begin{aligned} \mathcal{C}_{P,\vec{\kappa}} \quad = \quad & \{C' = (\vec{a}', \vec{b}', \vec{\alpha}', \vec{\beta}') \,:\, \vec{a}' = \vec{a}, \\ & \forall i,\, b'_i = a_i + d_i \pmod 3 \\ & \forall i \in E,\, \alpha'_i = \beta'_i \text{ and } \forall i \in S \setminus E,\, \alpha'_i = \neg\beta'_i \\ & K\alpha'_R = \vec{\kappa} \pmod 2, \\ & \text{where } S,\, E \text{ and } R \text{ are given by } \vec{d} \text{ and } \vec{e}.\}. \end{aligned}$$

Finally, we denote by $\mathcal{P}$ the set of all possible public announcements for which the validation test is passed. That is,

$$\mathcal{P} = \{P = (\vec{a}, \vec{d}, \vec{e}) \,:\, w_0(\vec{d}) \geq s \text{ and } e < \epsilon s\}.$$

We denote by T the subset $S \setminus (E \cup R)$, and by t the size of T.

Bell states

For each $i \in \{1 \dots n\}$, we define the Bell basis $\{|\,0\rangle_i, |\,1\rangle_i, |\,2\rangle_i, |\,3\rangle_i\}$ of the i-th pair of photons as:

$$\begin{aligned}
|\,0\rangle_i &= \frac{|\,0\rangle_{0,i}|\,1\rangle_{0,i} - |\,1\rangle_{0,i}|\,0\rangle_{0,i}}{\sqrt{2}},\\
|\,1\rangle_i &= \frac{|\,0\rangle_{0,i}|\,1\rangle_{0,i} + |\,1\rangle_{0,i}|\,0\rangle_{0,i}}{\sqrt{2}},\\
|\,2\rangle_i &= \frac{|\,0\rangle_{0,i}|\,0\rangle_{0,i} - |\,1\rangle_{0,i}|\,1\rangle_{0,i}}{\sqrt{2}},\\
|\,3\rangle_i &= \frac{|\,0\rangle_{0,i}|\,0\rangle_{0,i} + |\,1\rangle_{0,i}|\,1\rangle_{0,i}}{\sqrt{2}},
\end{aligned}$$

where the first and the second state in the product states in the rhs. correspond to Alice's and Bob's i-th photon's polarisation state, respectively.

Given a basis $a \in \{0,1,2\}$, we define X_a as the set of indexes of Bell states that are compatible with Alice and Bob measuring in the same basis a and obtaining opposite bit values (corresponding to a faithful transmission, as the source is supposed to emit an antisymmetric state). Likewise, we define Y_a as the set of indexes of Bell states that are compatible with Alice and Bob measuring in basis a and sharing the same bit value (corresponding to an error). That is, $X_0 = \{0,1\}$, $X_1 = \{0,2\}$, $X_2 = \{0,3\}$, $Y_0 = \{2,3\}$, $Y_1 = \{1,3\}$ and $Y_2 = \{1,2\}$. Given the choice of bases $\vec{a}$ and a set $A \subset \{1 \dots n\}$, we define X_{a_A} as $\{c_A \in \{0,1,2,3\}^A : \forall i \in A, c_i \in X_{a_i}\}$ and Y_{a_A} as $\{c_A \in \{0,1,2,3\}^A : \forall i \in A, c_i \in Y_{a_i}\}$. Given a reconciled set R and the choice of bases a_R on R, for any $c_R \in X_{a_R}$, we will denote by $\vec{\gamma}$ the unique $\vec{\gamma} \in \{0,1\}^r$ such that for each $i \in \{1, \dots, r\}$, $c_i = (1 + a_i)\gamma_i$. For any vectors $\vec{x}$, $\vec{y} \in \{0,1\}^r$, we define $\vec{x} \cdot \vec{y}$ as $\vec{x} \cdot \vec{y} \stackrel{Def}{=} \sum_{i=1}^{r} x_i y_i$. Given R and a_R, for any $c_R \in X_{a_R}$, we have the identity ${}_{a_R}\langle \alpha_R, \neg\alpha_R\,|c_R\rangle = \frac{(-1)^{\alpha_R \cdot (\neg\vec{\gamma})}(-i)^{\vec{\pi}_{a_R} \cdot \vec{\gamma}}}{\sqrt{2^r}}$, where $\vec{\pi}_{a_R}$ is a vector in $\{0,1\}^r$ with its i-th entry equal to 1 if and only if $a_i = 2$.

4.2 Model of measurements

The mathematical model of measurements on the quantum state generated by the source is almost identical to the one described in [1].

The state of the n couples of photons and the probe created by Eve reads as:

$$\rho = \sum_{\vec{c},\vec{c}'} |\,E_{\vec{c}}\rangle\langle E_{\vec{c}'}\,| \otimes |\,\vec{c}\rangle\langle\vec{c}'\,|,$$

where the states $|\,E_{\vec{c}}\rangle$ are states of Eve's probe that are possibly nor orthogonal nor normalised. The positive operator giving the probability that Alice and Bob get $C = (\vec{a}, \vec{b}, \vec{\alpha}, \vec{\beta})$ as their classical data is:

$$F_C = \mathrm{P}_{\mathfrak{a}}(\vec{a})\mathrm{P}_{\mathfrak{b}}(\vec{b})|\,\vec{\alpha}, \vec{\beta}\rangle_{\vec{a},\vec{b}\;\vec{a},\vec{b}}\langle\vec{\alpha}, \vec{\beta}\,|,$$

where $\mathrm{P}_{\mathfrak{a}}(\vec{a}) = 1/3^n$ and $\mathrm{P}_{\mathfrak{b}}(\vec{b}) = 1/3^n$ for any choice of $\vec{a}$ and $\vec{b}$. Note that since for all $i \in \{1 \ldots n\}$, $d_i = b_i - a_i \pmod 3$, we have $\mathrm{P}_{\mathfrak{a}}(\vec{a})\mathrm{P}_{\mathfrak{b}}(\vec{b}) = \mathrm{P}_{\mathfrak{a}}(\vec{a})\mathrm{P}_{\mathfrak{d}}(\vec{d})$ where $\mathrm{P}_{\mathfrak{d}}(\vec{d}) = 1/3^n$.

The positive operator giving the probability that Alice and Bob publicly announce $P = (\vec{a}, \vec{d}, \vec{e})$ while they get the private key $\vec{\kappa}$ is:

$$\begin{aligned} F_{P,\vec{\kappa}} &= \mathrm{P}_{\mathfrak{a}}(\vec{a})\mathrm{P}_{\mathfrak{d}}(\vec{d})\mathbf{1}_{\overline{S}} \otimes \sum_{\alpha_E \in \{0,1\}^e} |\, \alpha_E, \alpha_E \rangle_{a_E, a_E\ a_E, a_E} \langle \alpha_E, \alpha_E \,| \\ &\quad \otimes \sum_{\alpha_T \in \{0,1\}^t} |\, \alpha_T, \neg\alpha_T \rangle_{a_T, a_T\ a_T, a_T} \langle \alpha_T, \neg\alpha_T \,| \\ &\quad \otimes \sum_{\substack{\alpha_R \in \{0,1\}^r : \\ K\alpha_R = \vec{\kappa} \pmod 2}} |\, \alpha_R, \neg\alpha_R \rangle_{a_R, a_R\ a_R, a_R} \langle \alpha_R, \neg\alpha_R \,|, \end{aligned}$$

and the positive operator giving the marginal probability that Alice and Bob publicly announce $P = (\vec{a}, \vec{d}, \vec{e})$ is:

$$\begin{aligned} F_P &= \mathrm{P}_{\mathfrak{a}}(\vec{a})\mathrm{P}_{\mathfrak{d}}(\vec{d})\mathbf{1}_{\overline{S}} \otimes \sum_{\alpha_E \in \{0,1\}^e} |\, \alpha_E, \alpha_E \rangle_{a_E, a_E\ a_E, a_E} \langle \alpha_E, \alpha_E \,| \\ &\quad \otimes \sum_{\alpha_T \in \{0,1\}^t} |\, \alpha_T, \neg\alpha_T \rangle_{a_T, a_T\ a_T, a_T} \langle \alpha_T, \neg\alpha_T \,| \\ &\quad \otimes \sum_{\alpha_R \in \{0,1\}^r} |\, \alpha_R, \neg\alpha_R \rangle_{a_R, a_R\ a_R, a_R} \langle \alpha_R, \neg\alpha_R \,|. \end{aligned}$$

Note again that when no error occurs, Alice's bit and Bob's bit are anticorrelated.

We denote by $\mathcal{V}_P$ the set of views v that are compatible with the public announcement P. The positive operator giving the probability that Eve gets the view v given that Alice and Bob announced P will be denoted by $G_{v|P} = |\, \chi_{v|P} \rangle\langle \chi_{v|P} \,|$, where we assume again without loss of generality that the operators $G_{v|P}$ are of rank one.

4.3 The rôle of the validation test

Here a variation of the Property 2 in [1] is given. It is shown that when three bases are used for the validation test, the constraint on the photon state created by Eve is more stringent. Given a possible reconciled set R, let Π_R be the orthogonal projection operator defined as:

$$\begin{aligned} \Pi_R &= \sum_{\substack{\vec{c} \in \{0,1,2,3\}^n : \\ w(c_R) \geq d_K/2}} |\, \vec{c} \rangle\langle \vec{c} \,| \\ &= \mathbf{1}_{\overline{R}} \otimes \sum_{\substack{c_R \in \{0,1,2,3\}^r : \\ w(c_R) \geq d_K/2}} |\, c_R \rangle\langle c_R \,|. \end{aligned}$$

The following property is then proved.

Property 2 *The eigenvalues of the semi-definite positive Hermitian operator*

$$\sum_{P\in\mathcal{P}} \Pi_R F_P \Pi_R,$$

where R is specified by P in the sum, are bounded from above by

$$\theta(r) = e^{-\frac{1}{16}\tau^3 r}.$$

Proof The above operator can be written as:

$$\sum_{P\in\mathcal{P}} \Pi_R F_P \Pi_R = \sum_{\substack{\vec{d}\in\{0,1\}^n:\\ w_0(\vec{d})\geq s}} \sum_{\substack{\vec{e}\in\{0,1\}^s:\\ w(\vec{e})<\epsilon s}} \Pi_R \left(\sum_{\vec{a}} F_P\right) \Pi_R.$$

Now for given $\vec{d}$ and $\vec{e}$,

$$\sum_{\vec{a}} F_P = \mathrm{P}_{\mathfrak{d}}(\vec{d}) \mathbf{1}_{\overline{S}} \otimes_{i\in E} Y_i \otimes_{j\in T} X_j \otimes_{k\in R} X_k,$$

where

$$\begin{aligned} X_i &= |\,0\rangle\langle 0\,| + \frac{1}{3}|\,1\rangle\langle 1\,| + \frac{1}{3}|\,2\rangle\langle 2\,| + \frac{1}{3}|\,3\rangle\langle 3\,|, \\ Y_i &= \frac{2}{3}|\,1\rangle\langle 1\,| + \frac{2}{3}|\,2\rangle\langle 2\,| + \frac{2}{3}|\,3\rangle\langle 3\,| \end{aligned}$$

are operators acting on i-th photon pair's Hilbert space. The last equalities are derived directly from the definition of the Bell states. As a consequence, we have,

$$\Pi_R \left(\sum_{\vec{a}} F_P\right) \Pi_R = \mathrm{P}_{\mathfrak{d}}(\vec{d}) \mathbf{1}_{\overline{S}} \otimes_{i\in E} Y_i \otimes_{j\in T} X_j \otimes \Big(\sum_{\substack{c_R\in\{0,1,2,3\}:\\ w(c_R)\geq d_K/2}} \frac{|\,c_R\rangle\langle c_R\,|}{3^{w(c_R)}} \Big).$$

Now, given $\vec{d}\in\{0,1\}^n$, the operator:

$$\sum_{\vec{e}\,:\, w(\vec{e})<\epsilon s} \Pi_R \left(\sum_{\vec{a}} F_P\right) \Pi_R$$

is diagonal in the Bell basis $|\,\vec{c}\rangle$. Given a vector $\vec{c}\in\{0,1,2,3\}^n$ and an error vector $\vec{e}\in\{0,1\}^s$, a necessary condition for the scalar:

$$\langle\vec{c}\,|\Pi_R \left(\sum_{\vec{a}} F_P\right) \Pi_R |\,\vec{c}\rangle$$

to be non zero is that for all $i\in S$, $e_i = 0$ if $c_i = 0$ and $w(c_S) \geq \frac{d_K}{2} + e$. There are $\binom{w(c_S)}{e}$ such vectors $\vec{e}$ of weight e, if $0 \leq e < \epsilon s$ and $e \leq w(c_S) - d_K/2$.

Therefore,

$$\begin{aligned}
&\langle \vec{c}| \sum_{\vec{e}\,:\, w(\vec{e})<\epsilon s} \Pi_R \left(\sum_{\vec{a}} F_P \right) \Pi_R |\, \vec{c}\rangle \\
&\quad \leq \quad \mathrm{P}_{\mathfrak{d}}(\vec{d}) \sum_{\substack{0\leq e<\epsilon s \\ e\leq w(c_S)-d_K/2}} \binom{w(c_S)}{e} \left(\frac{2}{3}\right)^e \left(\frac{1}{3}\right)^{w(c_S)-e}.
\end{aligned}$$

Now, d_K is either greater or smaller than $\frac{2}{3}w(c_S)\,(1+\tau(1-\epsilon))$.

- If $d_K > \frac{2}{3}w(c_S)\,(1+\tau(1-\epsilon))$, then

$$w(c_S) - \frac{d_K}{2} < \frac{2}{3}w(c_S)\left(1-\frac{1}{2}\tau(1-\epsilon)\right) \text{ and,}$$

- if $d_K \leq \frac{2}{3}w(c_S)\,(1+\tau(1-\epsilon))$, then

$$\begin{aligned}
\epsilon s &\leq \frac{\epsilon r}{1-\epsilon} \\
&= d_K - \tau r \\
&\leq \frac{2}{3}w(c_S)\left(1-\frac{1}{2}\tau(1-\epsilon)\right),
\end{aligned}$$

where we have used $r \geq s(1-\epsilon)$ and $s \geq w(c_S)$.

We thus derived that:

$$\begin{aligned}
&\langle \vec{c}| \sum_{\vec{e}\,:\, w(\vec{e})<\epsilon s} \Pi_R \left(\sum_{\vec{a}} F_P \right) \Pi_R |\, \vec{c}\rangle \\
&\quad \leq \quad \mathrm{P}_{\mathfrak{d}}(\vec{d}) \sum_{0\leq e<\frac{2}{3}w(c_S)\left(1-\frac{1}{2}\tau(1-\epsilon)\right)} \binom{w(c_S)}{e} \left(\frac{2}{3}\right)^e \left(\frac{1}{3}\right)^{w(c_S)-e} \\
&\quad \leq \quad \mathrm{P}_{\mathfrak{d}}(\vec{d}) e^{-\frac{2}{9}\tau^2(1-\epsilon)^2 w(c_S)} \\
&\quad \leq \quad \mathrm{P}_{\mathfrak{d}}(\vec{d}) e^{-\frac{1}{16}\tau^3 r} \\
&\quad = \quad \mathrm{P}_{\mathfrak{d}}(\vec{d})\theta(r)
\end{aligned}$$

where we have used the binomial inequality stating that $\sum_{0\leq k<(p-t)n} \binom{n}{k} p^k (1-p)^{n-k} \leq e^{-2t^2 n}$ for any positive integer n and $0 < p - t \leq p < 1$. In the last inequality we have used the inequalities $\epsilon < 1/4$ and $w(c_S) \geq d_K/2$ when the above scalar is non zero.

Remarking that the operator $\sum_{\vec{a},\vec{e}\,:\ e<\epsilon s} \Pi_R F_P \Pi_R$ is diagonal in the Bell basis for all $\vec{d}$ and $\sum_{\vec{d}\,:\, w_0(\vec{d})\geq s} \mathrm{P}_{\mathfrak{d}}(\vec{d}) \leq 1$, this concludes the proof. □

The above property implies that:

$$\mathrm{Tr}\Big(\mathbf{1}_{\mathrm{Eve}} \otimes \sum_{P\in\mathcal{P}} \Pi_R F_P \Pi_R \rho\Big) \leq \theta(r)$$

where $\mathbf{1}_{\mathrm{Eve}}$ is the identity operator acting on the Hilbert space of the probe. That is,

$$\sum_{P\in\mathcal{P}} \mathrm{P}_{\mathsf{a}}(\vec{a})\mathrm{P}_{\mathsf{d}}(\vec{d}) \sum_{\substack{c_{\overline{R}}:\\ c_E\in Y_{a_E},\\ c_T\in X_{a_T}}} \sum_{\substack{c_R\in X_{a_R}:\\ w(c_R)\geq d_K/2}} \langle E_{\vec{c}}\,|\,E_{\vec{c}}\rangle \leq \theta(r).$$

4.4 Quasi-independence of the key and the view

In this section we compute the joint probability distribution of the key and the view. We prove that this distribution is very close to a product of an uniform distribution for the key and the marginal probability distribution of the view. This section is identical to the Section 5.4 of the previous proof, except for the apparition of few phase factors that do not appear in the final result.

Property 3 *For any given eavesdropping strategy chosen by Eve and returning a view $\boldsymbol{v}$, the probability distribution of the key $\vec{\boldsymbol{\kappa}}$ and the view $\boldsymbol{v}$ obeys the following inequality:*

$$\sum_{P\in\mathcal{P}}\sum_{v\in\mathcal{V}_P}\sum_{\vec{\kappa}\in\{0,1\}^m}\left|\mathrm{P}_{\sim\mathsf{v}}(\vec{\kappa},v)-\frac{1}{2^m}\mathrm{P}_{\mathsf{v}}(v)\right| \leq 2\left(\theta(r)+2\sqrt{\theta(r)}\right)$$

where m is the length of the private key and r is the size of the reconciled set.

Proof For any $\vec{\kappa}\in\{0,1\}^m$, P and $v\in\mathcal{V}_P$, we have:

$$\begin{aligned}
&\mathrm{P}_{\sim\mathsf{v}}(\vec{\kappa},v)-\frac{1}{2^m}\mathrm{P}_{\mathsf{v}}(v)\\
&\quad= \mathrm{Tr}(G_{v|P}\otimes F_{P,\vec{\kappa}}\,\rho)-\frac{1}{2^m}\mathrm{Tr}(G_{v|P}\otimes F_P\,\rho)\\
&\quad= \mathrm{P}_{\mathsf{a}}(\vec{a})\mathrm{P}_{\mathsf{d}}(\vec{d}) \sum_{\substack{\vec{c},\vec{c}'\,:\\ c_E,c'_E\in Y_{a_E},\\ c_T,c'_T\in X_{a_T},\\ c_R,c'_R\in X_{a_R}}} \langle E_{\vec{c}'}\,|G_{v|P}|\,E_{\vec{c}}\rangle\delta_{c_{\overline{R}},c'_{\overline{R}}}d_{\vec{\kappa},a_R}(\vec{\gamma},\vec{\gamma}'),
\end{aligned}$$

where

$$d_{\vec{\kappa},a_R}(\vec{\gamma},\vec{\gamma}')=(-i)^{\vec{\pi}_{a_R}\cdot\vec{\gamma}}(+i)^{\vec{\pi}_{a_R}\cdot\vec{\gamma}'} \sum_{\substack{\alpha_R\in\{0,1\}^r:\\ K\alpha_R=\vec{\kappa}\pmod 2}} \frac{(-1)^{\alpha_R\cdot(\vec{\gamma}+\vec{\gamma}')}}{2^r}-\frac{1}{2^m}\delta_{\vec{\gamma},\vec{\gamma}'}.$$

where we have used the identity ${}_{a_R,a_R}\langle\alpha_R,\neg\alpha_R\,|c_R\rangle = \frac{(-1)^{\alpha_R\cdot(\neg\vec{\gamma})}(-i)^{\vec{\pi}_{a_R}\cdot\vec{\gamma}}}{\sqrt{2^r}}$ for any $c_R\in X_{a_R}$ (note that $\neg\vec{\gamma}+\neg\vec{\gamma}'=\vec{\gamma}+\vec{\gamma}'$).

Let's define $\mathcal{G}$ as the set of all linear combinations over $\{0,1\}$ of rows of K. It has been proved in [1] that:

$$\sum_{\substack{\alpha_R\in\{0,1\}^r:\\ K\alpha_R=\vec{\kappa}\pmod 2}} (-1)^{\alpha_R\cdot(\vec{\gamma}+\vec{\gamma}')} = \begin{cases} (-1)^{\vec{\theta}_{\vec{\kappa}}\cdot(\vec{\gamma}+\vec{\gamma}')}2^{r-m} & \text{if } \vec{\gamma}+\vec{\gamma}'\in\mathcal{G},\\ 0 & \text{if } \vec{\gamma}+\vec{\gamma}'\notin\mathcal{G}\end{cases}$$

where $\vec{\theta}_{\vec{\kappa}}$ is a vector in $\{0,1\}^r$ such that $K\vec{\theta}_{\vec{\kappa}} = \vec{\kappa} \pmod 2$. We have:

$$\mathrm{P}_{\sim \mathsf{v}}(\vec{\kappa}, v) - \frac{1}{2^m}\mathrm{P}_{\mathsf{v}}(v) = \frac{1}{2^m}\mathrm{P}_{\mathfrak{a}}(\vec{a})\mathrm{P}_{\mathfrak{d}}(\vec{d}) \sum_{\substack{c_{\overline{R}}: \\ c_E \in Y_{a_E}, \\ c_T \in X_{a_T}}} (U_{v\vec{\kappa}c_{\overline{R}}} + V_{v\vec{\kappa}c_{\overline{R}}})^\dagger \Delta (U_{v\vec{\kappa}c_{\overline{R}}} + V_{v\vec{\kappa}c_{\overline{R}}}),$$

where $U_{v\vec{\kappa}c_{\overline{R}}}$ and $V_{v\vec{\kappa}c_{\overline{R}}}$ are complex vectors of dimension 2^r and Δ is a $2^r \times 2^r$ complex matrix, whose entries are indexed by $\vec{\gamma} \in \{0,1\}^r$. The $\vec{\gamma}$-th entry of $U_{v\vec{\kappa}c_{\overline{R}}}$ and $V_{v\vec{\kappa}c_{\overline{R}}}$ are:

$$\Big(U_{v\vec{\kappa}c_{\overline{R}}}\Big)_{\vec{\gamma}} = \begin{cases} (-1)^{\vec{\theta}_{\vec{\kappa}}\cdot\vec{\gamma}}(-i)^{\vec{\pi}_{a_R}\cdot\vec{\gamma}}\langle\chi_{v|P}\,|E_{\vec{c}}\rangle & \text{if } w(\vec{\gamma}) < d_K/2, \\ 0 & \text{if } w(\vec{\gamma}) \geq d_K/2. \end{cases}$$

$$\Big(V_{v\vec{\kappa}c_{\overline{R}}}\Big)_{\vec{\gamma}} = \begin{cases} 0 & \text{if } w(\vec{\gamma}) < d_K/2, \\ (-1)^{\vec{\theta}_{\vec{\kappa}}\cdot\vec{\gamma}}(-i)^{\vec{\pi}_{a_R}\cdot\vec{\gamma}}\langle\chi_{v|P}\,|E_{\vec{c}}\rangle & \text{if } w(\vec{\gamma}) \geq d_K/2, \end{cases}$$

where $\vec{c}$ is given by $c_{\overline{R}}$ and $\vec{\gamma}$. The $(\vec{\gamma}, \vec{\gamma}')$-th entry of Δ is, as in [1]:

$$\Big(\Delta\Big)_{\vec{\gamma},\vec{\gamma}'} = \begin{cases} 1 & \text{if } \vec{\gamma} + \vec{\gamma}' \in \mathcal{G} \setminus \{0\}, \\ 0 & \text{if } \vec{\gamma} + \vec{\gamma}' \notin \mathcal{G} \setminus \{0\}. \end{cases}$$

This implies $U^\dagger_{v\vec{\kappa}c_{\overline{R}}}\Delta U_{v\vec{\kappa}c_{\overline{R}}} = 0$, since $w(\vec{\gamma}) < d_K/2$ and $w(\vec{\gamma}') < d_K/2$ implies that $w(\vec{\gamma} + \vec{\gamma}') < d_K$, that is, $\vec{\gamma} + \vec{\gamma}' \notin \mathcal{G} \setminus \{\vec{0}\}$. The matrix Δ is diagonalised in the same manner as in [1], and we obtain:

$$V^\dagger_{v\vec{\kappa}c_{\overline{R}}}\Delta V_{v\vec{\kappa}c_{\overline{R}}} = 2^m\Big[(2^m-1)\sum_{\vec{x}\in\mathcal{S}}|\psi_{v,c_{\overline{R}},\vec{x},\vec{\kappa}}|^2 - \sum_{\substack{\vec{x}\in\mathcal{S} \\ \vec{\sigma}\in\{0,1\}^m\setminus\vec{0}}} |\psi_{v,c_{\overline{R}},\vec{x},\vec{\kappa}+\vec{\sigma}}|^2\Big],$$

$$U^\dagger_{v\vec{\kappa}c_{\overline{R}}}\Delta V_{v\vec{\kappa}c_{\overline{R}}} = 2^m\Big[(2^m-1)\sum_{\vec{x}\in\mathcal{S}}|\phi^*_{v,c_{\overline{R}},\vec{x},\vec{\kappa}}\psi_{v,c_{\overline{R}},\vec{x},\vec{\kappa}}| - \sum_{\substack{\vec{x}\in\mathcal{S} \\ \vec{\sigma}\in\{0,1\}^m\setminus\vec{0}}} |\phi^*_{v,c_{\overline{R}},\vec{x},\vec{\kappa}+\vec{\sigma}}\psi_{v,c_{\overline{R}},\vec{x},\vec{\kappa}+\vec{\sigma}}|\Big].$$

where $\mathcal{S}$ is a subspace of $\{0,1\}^r$ supplement to $\mathcal{G}$, and for any $\vec{z} \in \{0,1\}^m$,

$$\phi_{v,c_{\overline{R}},\vec{x},\vec{z}} = \sum_{\substack{\vec{y}\in\mathcal{G}: \\ w(\vec{x}+\vec{y})<d_K/2}} (-i)^{\vec{\pi}_{a_R}\cdot\vec{y}}\frac{(-1)^{\vec{\omega}_{\vec{y}}\cdot\vec{z}}}{2^m}\langle\chi_{v|P}\,|\,E_{\vec{c}}\rangle,$$

$$\psi_{v,c_{\overline{R}},\vec{x},\vec{z}} = \sum_{\substack{\vec{y}\in\mathcal{G}: \\ w(\vec{x}+\vec{y})\geq d_K/2}} (-i)^{\vec{\pi}_{a_R}\cdot\vec{y}}\frac{(-1)^{\vec{\omega}_{\vec{y}}\cdot\vec{z}}}{2^m}\langle\chi_{v|P}\,|\,E_{\vec{c}}\rangle.$$

where for any $\vec{y} \in \mathcal{G}$, $\vec{\omega}_{\vec{y}}$ is the unique vector in $\{0,1\}^m$ such that $K^T\vec{\omega}_{\vec{y}} = \vec{y} \pmod 2$.

From this one derives the inequality:

$$\sum_{P\in\mathcal{P}}\sum_{v\in\mathcal{V}_P}\sum_{\vec{\kappa}\in\{0,1\}^m}\left|\mathrm{P}_{\sim\mathsf{v}}(\vec{\kappa}, v) - \frac{1}{2^m}\mathrm{P}_{\mathsf{v}}(v)\right| \leq 2(2^m-1)(\eta + 2\sqrt{\eta}\sqrt{\xi}),$$

where

$$\eta = \sum_{P\in\mathcal{P}} \sum_{\substack{c_{\overline{R}}:\\ c_E\in Y_{a_E},\\ c_T\in X_{a_T}}} \sum_{v\in\mathcal{V}_P}\sum_{\vec{x}\in\mathcal{S}}\sum_{\vec{\kappa}} \mathrm{P}_{\mathsf{a}}(\vec{a})\mathrm{P}_{\mathsf{d}}(\vec{d})|\psi_{v,c_{\overline{R}},\vec{x},\vec{\kappa}}|^2,$$

$$\xi = \sum_{P\in\mathcal{P}} \sum_{\substack{c_{\overline{R}}:\\ c_E\in Y_{a_E},\\ c_T\in X_{a_T}}} \sum_{v\in\mathcal{V}_P}\sum_{\vec{x}\in\mathcal{S}}\sum_{\vec{\kappa}} \mathrm{P}_{\mathsf{a}}(\vec{a})\mathrm{P}_{\mathsf{d}}(\vec{d})|\phi_{v,c_{\overline{R}},\vec{x},\vec{\kappa}}|^2.$$

We then derive an upper-bound on η and ξ. We have:

$$\begin{aligned}
\eta &= \sum_{P\in\mathcal{P}} \mathrm{P}_{\mathsf{a}}(\vec{a})\mathrm{P}_{\mathsf{d}}(\vec{d}) \sum_{\substack{c_{\overline{R}}:\\ c_E\in Y_{a_E},\\ c_T\in X_{a_T}}} \sum_{v\in\mathcal{V}_P}\sum_{\vec{x}\in\mathcal{S}} \sum_{\substack{\vec{y},\vec{y}'\in\mathcal{G}:\\ w(\vec{x}+\vec{y})\geq d_K/2\\ w(\vec{x}+\vec{y}')\geq d_K/2}} \sum_{\vec{\kappa}} \frac{(-1)^{\vec{\omega}_{\vec{y}+\vec{y}'}\cdot\vec{\kappa}}}{2^{2m}} \\
&\quad \times(-i)^{\vec{\pi}_{a_R}\cdot\vec{y}}(+i)^{\vec{\pi}_{a_R}\cdot\vec{y}'}\langle E_{\vec{c}'}\,|\,\chi_{v|P}\rangle\langle\chi_{v|P}\,|\,E_{\vec{c}}\rangle \\
&= \frac{1}{2^m}\sum_{P\in\mathcal{P}} \mathrm{P}_{\mathsf{a}}(\vec{a})\mathrm{P}_{\mathsf{d}}(\vec{d}) \sum_{\substack{c_{\overline{R}}:\\ c_E\in Y_{a_E},\\ c_T\in X_{a_T}}} \sum_{\vec{x}\in\mathcal{S}} \sum_{\substack{\vec{y}\in\mathcal{G}:\\ w(\vec{x}+\vec{y})\geq d_K/2}} \sum_{v\in\mathcal{V}_P} \langle E_{\vec{c}}\,|\,\chi_{v|P}\rangle\langle\chi_{v|P}\,|\,E_{\vec{c}}\rangle \\
&\leq \frac{1}{2^m}\theta(r),
\end{aligned}$$

using the result of the previous section. Similarly,

$$\xi \leq \frac{1}{2^m}.$$

Consequently,

$$\begin{aligned}
&\sum_{P\in\mathcal{P}}\sum_{v\in\mathcal{V}_P}\sum_{\vec{\kappa}\in\{0,1\}^m}\left|\mathrm{P}_{\sim\mathsf{v}}(\vec{\kappa},v)-\frac{1}{2^m}\mathrm{P}_{\mathsf{v}}(v)\right| \\
&\quad\leq\ 2\left(\theta(r)+2\sqrt{\theta(r)}\right)
\end{aligned}$$

which concludes our proof. □

4.5 Bound on the conditional entropy

As in [1], we conclude the proof of privacy thanks to the following property.

Property 4 *Let $\boldsymbol{x}$ and $\boldsymbol{y}$ be two discrete random variables taking values in the sets $\mathcal{X}$ and $\mathcal{Y}$ respectively. Let μ be a nonnegative real number. If the following inequality is satisfied:*

$$\sum_{x\in\mathcal{X},\,y\in\mathcal{Y}}\left|\mathrm{P}_{\mathsf{xy}}(x,y)-\frac{1}{|\mathcal{X}|}\mathrm{P}_{\mathsf{y}}(y)\right|\leq\mu,$$

then the conditional entropy of $\boldsymbol{x}$ *given* $\boldsymbol{y}$ *is lower-bounded by:*

$$H(\boldsymbol{x}|\boldsymbol{y}) \geq (1-\mu)\log_2|\mathcal{X}| - \frac{1}{\ln 2}\mu.$$

The proof of this property has been given in [1]. The probability distribution of the private key and the view obeys the inequality:

$$\sum_{\substack{\vec{\kappa}\in\{0,1\}^m,\\ v\in\mathcal{V}}} \left|\mathrm{P}_{\sim \mathsf{v}}(\vec{\kappa},v) - \frac{1}{2^m}\mathrm{P}_{\mathsf{v}}(v)\right| \leq 2(\theta(r)+2\sqrt{\theta(r)}),$$

where we have used the fact that the key is randomly chosen by Alice with uniform probability distribution if the validation test is not passed. Applying the above property for the random variables $\vec{\boldsymbol{\kappa}}$ and $\boldsymbol{v}$, we obtain:

$$H(\vec{\boldsymbol{\kappa}}|\boldsymbol{v}) \geq m - 2\left(m+\frac{1}{\ln 2}\right)\left(\theta(r)+2\sqrt{\theta(r)}\right),$$

which concludes the proof of privacy. □

Acknowledgements The author gratefully acknowledges support provided by the European TMR Network ERP-4061PL95-1412, and thanks Hans Briegel, Artur Ekert, Nicolas Gisin, Patrick Hayden, Norbert Lütkenhaus, Dominic Mayers, Michele Mosca, Luke Rallan, Peter Shor and Vlatko Vedral for interesting discussions and helpful comments.

References

[1] H. Inamori. Security of EPR-based quantum key distribution. quant-ph/0008064, 2000.

[2] D. Bruß. Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.*, 81:3018, 1998.

[3] H.-K. Lo. A simple proof of the unconditional security of quantum key distribution. quant-ph/9904091, 1999.